
FRAUD IN ACCOUNTS PAYABLE

HOW TO PREVENT IT



by Mary S. Schaeffer
Editorial Director

Accounts Payable Now & Tomorrow, a CRYSTALLUS, Inc. Publication

Sponsored by BasWare Inc.

© 2007 Mary S. Schaeffer and CRYSTALLUS, Inc.

Reproduction without expressed permission from Mary S. Schaeffer is prohibited.

Accounts Payable Now & Tomorrow does not render legal, accounting, or other professional services. Legal and other expert assistance should be sought from competent professionals.

www.ap-now.com

560 Peoples Plaza #560, Newark, DE 19702

For information about reprints, or other publishing or consulting matters, contact
publisher@ap-now.com or call 302.836.0540

Table of Contents

Introduction	5
Common Myths about Fraud	5
Types of Fraud	6
Payment Fraud: Overview	6
Check Fraud	7
Why It's Everyone's Problem	7
Who's Responsible for Check Fraud Losses?	7
Check Fraud Prevention Practices	8
Check Fraud Prevention: Types of Positive Pay	9
ACH Payment Fraud	10
Background: How ACH Payments Work	10
ACH Fraud Prevention	11
Employee (Occupational) Fraud	12
Employee Fraud: P-cards	12
Travel & Entertainment (T&E) Reimbursement Fraud	13
How Big Is the T&E Fraud Problem?	13
T&E Fraud: Policy for Small-Dollar Offenses	14
What about Spot-checking	15
Vendor Fraud: Phony Invoices	15
Phony Invoices: Controls	15
Vendor Fraud: Invoices	16
Vendor Fraud: Solutions	16
Technology's Role in Fraud Prevention	17
Audit Trails	17
Online Three-Way Matching	17
Travel and Entertainment	18
Master Vendor File	18
Reporting	18
Actual vs. Budget	19

In Conclusion	19
An Ounce of Prevention: Overall Fraud Prevention Guidelines	19
Closing Thoughts	20
Additional Resources	20
Appendices	
Appendix 1: Blank Check Stock Security Features	21
Appendix 2: About Mary Schaeffer	22
Appendix 3: About Accounts Payable Now & Tomorrow and CRYSTALLUS, Inc.	22
Appendix 4: About our Sponsor: BasWare Inc.	

Introduction

It's an incontrovertible fact of corporate life; fraud happens. Accounts payable is particularly vulnerable for a very simple reason: it is where access to the organization's money lies. And since accounts payable is responsible for most payment functions, it falls to those in charge to ensure the tightest possible controls around everything affecting the disbursement function.

Common Myths about Fraud

Organizations are often lulled into a false sense of complacency regarding fraud because of several myths. Then when it does happen and there is a loss, everyone is horrified. Let's take a look at some of the misconceptions that get companies in trouble.

Myth: Fraud would never happen here; it's something that happens at other companies.

Fact: Crooks don't discriminate. They'll steal from whomever they can, taking advantage of any weakness. Occasionally, companies believe they are too small for a crook to be interested in their money—only to find they are 100% wrong. Sharks smell an opening wherever one exists.

Myth: Check fraud is not a problem because we use Positive Pay and pay electronically.

Fact: While paying electronically may reduce an organization's exposure to check fraud somewhat, that's all it does. And that doesn't mean the organization won't be subject to ACH or electronic payment fraud. Finally, unless an organization is using the newest form of Positive Pay, Payee (name) Positive Pay, the product only partially protects the user from check fraud.

Myth: My bank will eat any losses due to check fraud. **Fact:** While this may have been true ten or fifteen years ago, it is no longer the case. Banks simply cannot afford to eat all the check fraud losses—especially if they are large. Changes in the Uniform Commercial Code (UCC) have addressed this issue. This is not to say that occasionally a bank won't take care of a small-dollar loss for a large and valued customer but it is a terrible idea to think of your bank as insurance against check fraud losses.

At the other end of the spectrum, there are companies that do not take advantage of some of the best payment methodologies because of distrust. It is not uncommon to hear an executive refuse to have purchase cards in their organization for fear the employees, if given credit cards, would rob the organization blind. There are two responses to this claim. First, although p-card fraud does occur, it is rare. And, more to the point, why would an organization have employees working for it that it did not trust?

Types of Fraud

Obviously, there are many types of fraud—and virtually all result in a financial loss for the organization. For the purposes of this paper we will focus on those that fall under the umbrella of accounts payable.

Payment fraud falls into two broad categories:

- ◆ Check fraud is the set of crimes related to altering or creating a paper check with the intent of defrauding the paying organization of funds. This can include the complete fabrication of a fake check or the alteration of a legitimate check by either changing the payee or the dollar amount. Recently there has been a shift towards payee name alteration and away from changing the dollar amount due to the introduction of Positive Pay.
- ◆ ACH (electronic payments through the Automated Clearing House) fraud exists although not nearly to the level of check fraud. As the payment mechanism of choice continues to move away from paper, this type of fraud will increase. It is important for those reading this to understand they are vulnerable to this type of fraud regardless of whether or not they actively make electronic payments. This exposure makes it imperative that everyone takes action to protect themselves, not just those participating in the electronic payment marketplace.

Employee fraud occurs because employees, especially those working in the finance and accounting functions, are very familiar with an organization's payment processes and know their Achilles' heels. Thus, if they are so inclined, they are uniquely positioned to take advantage of these weaknesses.

Vendor fraud can hit your organization from both legitimate vendors and complete strangers. The issues break down into two categories:

- ◆ Fraudulent invoices—those that thieves send for items you never ordered; and
- ◆ The gray area—the legitimate invoices with charges you did not agree to or with inflated prices. Some of these inaccuracies may be due to miscommunication or honest human errors, or they may represent an attempt on the part of a shoddy vendor to get a higher price than originally negotiated. Discerning the difference can be next to impossible.

Payment Fraud: Overview

Checks still make up the dominant share of problems when it comes to payment fraud. Just a few short years ago we would not have addressed other types of payment fraud but given the advances in the payment world that is changing.

Today it is critical that all organizations put controls in place to prevent electronic payment fraud even if they have no electronic payment programs in operation. The reason for this is simple. Swindlers will try to extract money from your bank accounts in any way they can and a number have figured out how to at your accounts without writing a check. Thus we caution *everyone* to read the sections on electronic payment fraud prevention.

Check Fraud

Why It's Everyone's Problem

As mentioned earlier, banks are no longer willing to eat losses associated with check fraud, especially if the loss is due to negligence on the part of your organization. In 1990, the Uniform Commercial Code (UCC) was changed and the concepts of ordinary care and comparative negligence were introduced. These concepts are used to determine liability if a check fraud occurs. With check fraud continuing to skyrocket, every organization needs to fully understand their responsibilities.

In 1993 reported check fraud totaled \$5 billion. In 1996, that figure rose to \$12 billion. The check fraud problem now is substantially larger than it was in 1993, and remember that was after the UCC was changed. According to figures from the Nilson Report in 2003, check fraud exceeded \$20 billion per year. Looking at these numbers, it's easy to understand why banks have had enough and companies are taking aggressive steps to protect themselves.

There have been more than a few instances where a bank and a large corporate client parted ways when the bank refused to eat check fraud losses resulting from the corporate client's negligence.

Who's Responsible for Check Fraud Losses?

There are three parties to be considered when assessing responsibility for a check fraud loss:

1. The party that issued the check (your company);
2. The bank of first deposit; and

The collecting bank.

The idea is that each party operates in a manner that minimizes the possibility for check fraud. In Articles Three and Four, the UCC describes the responsibilities needed under the concepts of ordinary care and comparative negligence. Generally speaking, the losses associated with a check fraud are allocated to the parties (listed above) sharing the responsibility for the prevention of the check fraud. The allocation depends on the parties' ability to prevent the fraud. In other words, it depends on the amount of contributory negligence assessed to each party. In such discussions "contributory negligence" is the constant refrain.

The other factor is the concept called ordinary care. This requires that customers follow "reasonable commercial standards" for their industry or business. This seemingly innocuous statement can have significant ramifications—so don't overlook it. An organization's failure to exercise ordinary care is considered to have substantially contributed to the fraud. Or to put it another way, they are deemed to have neglected their obligation to exercise ordinary care.

This brings us to the subject of Positive Pay and what happens if you refuse to use it. You are probably aware that most experts identify Positive Pay as the single best defense against check fraud. If your organization is not using Positive Pay, you may have unwittingly given up your some of you protections against fraud losses.

Ask to see the deposit agreement to ensure the bank has not passed the liability to your organization. Claiming ignorance will get you nowhere if a fraudulent check makes it through the system. Even if there is nothing in the deposit agreement, you might inquire of the treasurer, controller, or whoever is responsible for banking relationships if the firm ever signed a letter refusing to accept Positive Pay. Some banks require this and use it as a defense to shift payment responsibility to their customers in cases of check fraud.

It should be noted that the UCC does not specifically define reasonable care. But not using Positive Pay is considered by many as not exercising reasonable care.

If you haven't recently taken a look at the controls around your check stock or your processes and controls around checks while they are being signed and mailed, you might want to do so. You might be flabbergasted at what you find.

Use of a rubber stamp to sign checks negates any defense you might have if your checks are forged. Luckily, few organizations still make use of such a devise.

Check Fraud Prevention Practices

When it comes to check fraud, you can't be too careful. As stated earlier, use of Positive Pay is probably the single best step you can take to protect your organization when it comes to check fraud. Additionally recommended are strong internal controls regarding:

- ◆ Storage of check stock;
- ◆ Control of checks from printing through mailing; and

Incorporation of at least three safety features in check stock (see Appendix 1 for a list of some of the features currently offered by printers).

Don't overlook the appropriate segregation of duties within the organization when it comes to the check production process either. The more people involved in the check production

cycle, the more difficult it is to commit internal check fraud. By this we mean that if the task is divided into many different segments with a different individual responsible for each, it becomes more difficult for an unscrupulous employee to commit fraud without collaboration. Of course this is difficult to do in smaller departments.

As for the storage of check stock, the issue is more of a concern if you use preprinted check stock instead of laser checks, where all the pertinent information is printed on the check at one time. Still, many guard their check stock carefully as it makes it all the harder for the internal cheat to commit fraud if they cannot get their hands on check stock easily.

Check Fraud Prevention: Types of Positive Pay

There are a number of variations of Positive Pay on the market. Most were developed as crooks found ways around the original models developed. Here's a look at what's available today.

♣ **The Basic Model:** The basic Positive Pay model requires that a company send a file to the bank each time it does a check run. The file contains numbers and dollar amounts of all checks issued. The bank then matches all checks that come in for clearing against this file. Once a check comes in and is paid, the item is removed from the file and cannot be paid again.

This approach takes a big whack at the check fraud problem. It eliminates several huge check fraud issues including:

- Copying one check numerous times and the subsequent cashing of all of them;
- The altering of the dollar amount on a check; and
- The complete manufacture of fraudulent checks drawn on an organization's bank account.

What the basic model does not address are checks cashed by tellers and those where the payee's name is changed. Additionally, companies that could not produce a check-issued file for transmission to their banks are left unprotected. And, as might be expected, once criminal elements got wind of Positive Pay, some adjusted their sights focusing on checks cashed at teller windows and changing the payee's name rather than the dollar amount. But before we look at the products that address those issues, let's take a look at the banks' response for those companies that could not produce a check-issued file.

♣ **Reverse Positive Pay:** Recognizing that not every organization was able or willing to produce the tape needed for Positive Pay, banks introduced another service. It's called reverse because it reverses the process. Each morning the bank tells the company what checks have been presented for clearing. It is up to the company to check those listings and make sure that they are all legitimate. Typically, there is a fall-back position if the company does not notify the bank and usually that is that the bank pays on the check. The action

should be discussed with the bank when the reverse Positive Pay relationship is initially set up.

♣ **Teller Positive Pay:** Once it became obvious checks were being verified before they were honored, pilferers realized that most tellers did not have this information and started cashing phony checks in person. Some banks now make this information available to their tellers on the platforms. If your bank is one of these, ask how frequently this information is updated. Some update continuously while others only update this information overnight. If it is only overnight, you could have some angry or annoyed vendors or employees on your hands if they try to cash their checks on the same day they are issued. A phone call usually takes care of these situations.

♣ **Payee Name Positive Pay:** Recognizing that fraudsters were reduced to focusing their efforts on changing the payee names on checks, a few banks have taken up the fight in that regard. In addition to the check number and dollar amount, they will also verify the payee name.

ACH Payment Fraud

Background: How ACH Payments Work

ACH payments can either be debits or credits. An organization can either initiate the payment itself or allow the payee to do so. If it sends its bank the appropriate information to make the payment, an ACH credit has occurred. On the other hand, if you provide your banking information to your supplier and allow the supplier to initiate the payment taking the funds from your account, an ACH debit transaction has occurred.

While the net result is the same, not everyone is comfortable in allowing vendors to debit their accounts. In fact, this is most likely to occur if a taxing authority is involved or if there is a captive relationship between the vendor and the customer.

Most organizations that do allow debits from their accounts only do so on a very limited basis. They also generally set up a separate account just for this purpose.

Real-life examples of ACH credits include direct deposit of payroll and social security payments. In fact, this analogy has led to the use of the term direct payments to refer to electronic payments.

Probably the most common example in the consumer world of ACH debits are those transactions related to mortgages, where the mortgage company takes the payment out of the consumer's account once a month, usually at the beginning. In the B2B world, ACH debits are sometimes used to pay sales and use tax obligations, rent, and occasionally by service stations to pay for gas deliveries or goods for the onsite convenience shops.

As you can see, if a thief has the appropriate information it is relatively easy for him or her to initiate an ACH debit. There's no need to dirty one's hands going into the bank and trying to cash a check. It is for this reason that it is so important that everyone put ACH blocks on accounts where debits will not be allowed.

It is also why it's a good reason to set up a separate account for ACH debits. Otherwise, anyone who gets a check from you has all the information needed to initiate a debit.

ACH Fraud Prevention

One or more of the following products can be beneficial in protecting your organization.

♣ ACH Blocks

ACH blocks allow organizations to notify their banks that ACH debits should not be allowed on certain accounts. With this in place no ACH debit, even one that you authorize, will be able to get through on a given account. Organizations are advised to put these in place on all accounts where ACH activity is not likely to be used.

If you use this handy tool, however, remember to keep track of which accounts you've blocked. Otherwise, you could end up with egg on your face when a vendor is given authorization to use an ACH debit and everyone has forgotten that an earlier block was put on the account.

♣ ACH Filters

ACH filters allow organizations to give their banks a list of companies authorized to debit their accounts. The banks will then "filter" incoming debits and allow only those on the list. This filter does not check for dollar amounts or whether the particular transaction has been authorized, only that the company doing the debiting is on the approved list.

This product is sometimes referred to as ACH Positive Pay, although in this writer's mind this is really not the correct appellation. It can get even fuzzier because some banks match the identities of those attempting to debit an account with those on the list provided by the company and exceptions are reported to the customer to review before payment. Only authorized electronic transactions are permitted to go through.

♣ ACH Positive Pay

A robust Positive Pay product for the ACH environment is not universally available today—but it's on its way. And it comes at a time when the financial community is moving towards

payee name Positive Pay. Payee Positive Pay adds the payee name to the check-number and dollar-amount file transmitted to the financial institution. This became a necessity when swindlers figured out how to circumvent traditional Positive Pay products.

Employee (Occupational) Fraud

The Association of Certified Fraud Examiners (ACFE) in its Report to The Nation defines occupational fraud as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets."

Who commits employee fraud? Sadly, this is really ugly. According to the ACFE fraud is most commonly committed by:

- Long term trusted employees.
- Higher level employees with correspondingly higher losses.
- Males slightly more often than females.

And the news gets worse. The report details how fraud is uncovered as follows:

- Anonymous tips 34.9%
- Accidentally 25.4
- Internal audit 20.2
- Internal controls 19.2
- External audit 12.0
- Notified by police 3.8

As you can see, the corporate world does not do a great job either at preventing employee fraud or uncovering it. If a picture is worth 1000 words, the first number demonstrates in spades why having an anonymous hot line for tips is so important. Over one-third of the frauds are uncovered this way.

Employee Fraud: P-cards

The concern about fraud related to purchase cards used by employees is probably exaggerated. Yes there definitely have been instances, and some of them well publicized, but overall out-and-out p-card fraud happens rarely. This is not to say that the cards aren't sometimes used inappropriately but with proper instructions this can be rectified.

Stringent controls around the use of p-cards along with regular review are probably the best way to guard against fraud and misuse. Some of the controls include:

- Dollar limits on spend by occurrence and day.
- Limits by Merchant Category Code.
- Regular checking and approval of expenditures.

Every employee issued a card should sign a letter acknowledging their understanding that their employment can *and will* be terminated immediately if they are found using their cards inappropriately. And, as harsh as this may sound, if someone does use the card inappropriately for personal gain and they are dismissed, this fact should not be kept secret. It will serve as a deterrent against misuse by other employees. Just make sure the employee didn't make an honest mistake.

This brings up the question of whether the card can be used for personal use if the employee reimburses the organization for personal expenditures. Virtually every p-card program prohibits this although a few do allow personal expenditures on their travel and entertainment card.

Travel & Entertainment (T&E) Reimbursement Fraud

The first protection against T& E fraud is simple. A written policy disseminated to all affected parties heads off many problems. Sometimes, what might look like T&E fraud is simply miscommunication and an employee did not understand what is allowed under the corporate reimbursement policy. Since what is allowable varies greatly from one organization to the next, it is imperative that *all* employees be kept in the loop. The next recommended step is that the policy be enforced uniformly across all employees. This happens about 80% of the time. Without uniform policy enforcement, a company is hard-pressed when it comes to fraud allegations that are simply a little over the line.

Regarding the verification of reimbursement requests, spot-checking rather than verifying every receipt is generally recommended. However, there are two schools of thought:

- Don't spend a dollar to save a dime.
- Larger frauds are sometimes uncovered because the thief gets greedy and turns to the "easy" fraud: T&E.

How Big is the T&E Fraud Problem?

It's bigger than you might expect. Let's look at some numbers:

- In the ACFE's Report to the Nation, expense reimbursement fraud accounted for 14.2% of frauds reported in 2004, up from 12.2% in 2002.
- The cost wasn't insignificant with the median cost at \$60,000 in 2002 and \$92,000 in 2004.

The cost is so high because most of the frauds are ongoing with the employee stealing a little on each expense reimbursement request.

If you are wondering just how prevalent the problem is, consider this. In a recent *Accounts Payable Now & Tomorrow* survey of accounts payable professionals 38.03% of survey respondents had experienced some T&E fraud in the last three years. And those surveyed had been specifically instructed to exclude small-dollar frauds.

T&E Fraud: Policy for Small-Dollar Offenses

The first question is whether the reimbursement request questioning each case is an attempt to knowingly defraud the company or just an honest mistake. That's why it's so important to have a company policy that addresses all issues. The policy should be regularly updated and widely disseminated. Different companies will take different views as the following two real-life examples demonstrate:

♣ **Example 1:** Two women went to a conference requiring an overnight stay. It was their first business trip. When they went out for dinner, they noticed they got two receipts. So each of the women submitted the receipt requesting reimbursement for the entire amount, rather than her portion. The fraud in this example was less than \$100 with each woman receiving about half the amount.

♣ **Example 2:** A salesperson routinely added miles to every trip when requesting reimbursement for miles driven. When this fraud was uncovered, it was determined he had received an extra \$1300 over several years. When confronted with the facts by the organization's accounts payable manager the salesperson agreed with her figures but refused to reimburse the organization. When she got the controller involved, a payment plan was worked out and the salesperson agreed to repay the amount owed over the course of one year. He made one payment and refused to make additional payments. But, have no fear, the accounts payable manager deducted the funds when he put in for a large reimbursement for another matter. So ultimately, after much perseverance, the organization got its money.

Now here is the real killer. The employee(s) in only one of the examples was terminated. Before I tell you which one, think if you would have terminated either, both, or neither. If you guessed the women who put in for the extra meal were fired, you would be correct. When their chicanery was uncovered the company let both go and did not give them references. It should be noted that, while not an unreasonable outcome, most organizations would simply have demanded repayment.

What about Spot-checking?

Although spot-checking of submitted reimbursement requests is a recommended best practice, many organizations still check 100% of the returns. Those that spot-check typically examine somewhere between 5-20% of randomly selected reports plus known offenders and reports over a certain dollar level. Most accounts payable departments routinely review every reimbursement request submitted by individuals known to take creative license with their T&E reports, even if their policy is to only spot-check.

If using spot-checking it is recommended that a few individuals be selected (both randomly and from the suspected offender list) and all reports for the last 14 months be reviewed in tandem. Occasionally when this is done discrepancies pop up that are not otherwise obvious. For example, the same receipt may be used on more than one expense report. You might also notice receipts with sequential numbers indicating the employee is probably fabricating receipts for nonexistent expenditures.

Vendor Fraud: Phony Invoices

Be very alert for fraudulent small-dollar invoices for products never ordered. These frauds have been around for years and are ongoing. There is only one reason for that: they work. Many of the invoices involved are for small dollars. Thieves know it is not worth the time and effort for many organizations to research each invoice to determine if the goods were really ordered. They count on the fact that accounts payable staffs are overworked. Don't be drawn in and pay these invoices as it will only encourage more of the same. The most common of these schemes are fraudulent invoices for:

- Yellow pages ads;
- Help wanted ads;
- Inferior office supplier at inflated prices; and
- Toner cartridges.

Phony invoices: Controls

There's little you can do to prevent these invoices from being sent to you. However, you can and should take steps to make sure you don't pay them. Here are some of the steps to take:

- Require the name of the person who ordered the goods or the PO number be included on every invoice processed. Return any invoices without this information.
- Order office supplies only from a few approved suppliers.

- Never give copier information over the phone. It's the favorite way crooks start this scam.

Verify that all help wanted and yellow pages ad invoices are from legitimate concerns with which you normally do business, not some fly-by-night outfit whose material looks the same.

Vendor fraud: Invoices

Aside from the obviously fraudulent invoices, there is another category that causes concern. These are invoices from existing suppliers that seem to include an inordinate amount of errors, all in the vendor's favor. Is it fraud or an honest discrepancy? When faced with invoice after invoice from an existing supplier that is full of errors, you begin to wonder. Some of the issues include:

- ◆ Pricing discrepancies.
- ◆ Other fees (freight, insurance etc.) included incorrectly.
- ◆ Second invoices not marked copy or duplicate.
- ◆ Follow-up invoices with different invoice number.

If an invoice is not paid within 30 days, most vendors will send a second invoice. This increases the chances of a duplicate payment. These issues give rise to larger payments than negotiated and/or duplicate payments that are not returned. None of this is good for your company's balance sheet.

Vendor Fraud: Solutions

Whether it's fraud or a legitimate dispute, the impact to your bottom line is the same if you make a duplicate or erroneous payment. Here are a few tactics that take aim at the problem.

- Contract compliance.
- Use of electronic invoicing, resulting in quicker processing and fewer second invoices.
- Timely handling of invoices.
- Duplicate payment-checking routines before checks are released.
- Duplicate payment audits by third parties after the fact.

Duplicate payments are a fact of corporate life. Virtually every organization makes them. The goal should be to keep them to a minimum and if made to recover them. Most duplicate payment auditors work on a contingency basis; if they don't recover anything you owe them nothing. Some executives find it galling to pay for the recovery and refuse to hire the firms. To my mind this is foolish. Without the recovery firms, 100% of the money is lost. With

them, you get to put 75% of it back on your bottom line—and the better ones will help you close the loopholes in your processes that permitted the duplicate payments in the first place.

Technology's Role in Fraud Prevention

Clearly technology can play a huge role in preventing fraud related to accounts payable. Technology and automation also take the slack out of the processing making it possible for an invoice to be processed in a fraction of the time it would take for manual processing. Not only does this increase the throughput but it makes it more difficult for crooks relying on inefficient processes to sneak a fraudulent invoice through.

Automated processes can incorporate controls as well as allow the integration of simple and not-so-simple verifications during the process. For example, an automated process might allow you to incorporate levels of authorized spend with individuals submitting/approving invoices for payment. This could be done by title or by the person's name. If the person was not authorized to approve at the given level, the item in question could be automatically kicked up to the next level of authorizations without any human intervention.

Audit Trails

As those involved in accounting and the controllership functions are aware, audit trails are crucial. Software built especially for invoice processing and the procure-to-pay function leaves a clearly identifiable audit trail.

Depending on the product selected, it may be possible to identify every single person who touched a particular transaction. This might even include simply clicking on a link to view a transaction even if the individual did not alter the information or process it. This feature could serve as a deterrent to those who sneak around corporate files looking for information that might later be used to defraud the organization.

Online Three-Way Matching

Technology allows the automation of the proverbial three-way match (Invoices against purchase orders and receiving documents). All invoices that do not have the corresponding documents are kicked out for manual processing. Thus, the automation handles the bulk of the transactions leaving humans to focus their attention on the remaining. This will help highlight fraudulent invoices.

It should be noted that some organizations require a PO for every single purchase, These firms are in the minority but in these cases fraudulent invoices stick out like a sore thumb.

The automation of the three way match allows for detailed checking that is more difficult in a manual process.

Travel and Entertainment

Although the dollar amounts associated with travel and entertainment fraud are not always the largest, it is the place where employees can ding their employers the easiest if they are so inclined. Automated travel and entertainment policy compliance makes this difficult, if not impossible. Some of the travel and entertainment products have online policy compliance built in.

While the goal of these modules is generally to ensure employees are complying with the corporate policy, it also helps prevent T&E fraud. It should be noted that many employees who steal from their employers in other ways eventually cannot pass up the temptation to dip into the T&E fund. Many corporate frauds that have gone undetected come to light only after the perpetrator got greedy and tried to expand his or her thieving opportunities to T&E. Automated policy compliance checking is one way to catch this type of activity.

Master Vendor File

The master vendor file is often overlooked. Yet crafty employees who know how to manipulate entries to it can often swindle quite a bit from their employers. One easy way to determine whether this is going on under your watch is to take advantage of technology and run your employees' addresses against addresses of vendors in master vendor file. If you enter traveling employees as vendors for reimbursement purposes, remember to factor that fact into the equation.

Since some thieves use their home addresses (yes, even when they are stealing from their employers) this is a relatively easy way to identify potential fraud. Once you have the list of address matches, someone will need to review it and eliminate legitimate entries.

Reporting

With an automated process, data is usually accessible and can be analyzed in a variety of ways that may reveal fraudulent activity. For example, run reports showing:

- ✦ Number of voided checks by processor
- ✦ Number of exception items by processor
- ✦ Number of exception items by vendor
- ✦ Number of Rush checks by vendor
- ✦ Number of Rush checks by requisitioner

Number or checks returned to requisitioner by requisitioner

Use this data to identify potential trouble spots. This information will not only be useful in uncovering potential frauds but also in uncovering weak spots in your internal controls, employees who might need more training, requisitioners who are not approving invoices in a timely manner etc.

These are not the only reports you can run. Depending on the information in your database and your requirements, you will be able to devise numerous other reports to help with your fraud prevention and process improvements.

If you have purchased a software package for part or all of your procure-to-pay process, it may come with standard reports that will help uncover fraud. Take a serious look at all the reports offered. After all they are developed by real experts, the people who live and breathe technology and your application 24/7. They know what to look for and often have developed reports you will not think of. Take advantage of this expertise. It often comes as part of the package at no extra cost. Most organizations purchasing software use only a fraction of its capabilities. The reports you need may very well be there waiting for you to use them.

Actual vs. Budget

Many organizations spend a lot of time on the budgeting process and much less on reviewing budget vs. actual reports. This is unfortunate as what matters to the bottom line is the actual spend not the projected spend. Accounts payable has this information. By working with the data related to actual spend organizations may be able to:

- ✦ Negotiate better pricing discounts
- ✦ Negotiate better payment terms

Recover pricing discounts that were not taken due to a disjointed ordering process

The information needed for these negotiations lies in accounts payable. Mine the data and get the best deal you can for your organization. This data can be used to negotiate with a few preferred suppliers. In a large decentralized organization, local purchases are often made at prices that are not advantageous to the organization. On rare occasions the local purchasing professional receives kickbacks related to these overpriced transactions. Use of the data to negotiate favorable pricing puts an end to such unethical behavior.

In Conclusion

An Ounce of Prevention: Overall Fraud Prevention Guidelines

Here are a few guidelines to help keep your company's assets safe:

- Strong internal controls across all accounts payable, purchasing, accounting, and finance processes.
- Appropriate segregation of duties.
- Hot line or other mechanisms for truly anonymous reporting.
- Ethics training.

A policy manual so everyone knows his or her obligations. Then there can be no, "I didn't know that..." or, "You never told me we couldn't ..." or my favorite, "At my old company we ..." (I'm always amazed at what was allowed at "the old company.")

Closing Thoughts

Crooks and fraud are here to stay. They've been around forever. Many are quite crafty while a number of them are almost as stupid as they are lazy. They're the easy ones to catch. Unfortunately, the smart ones rarely get caught and keep at it. (There's also the issue of the lack of meaningful punishment for most white-collar criminals—but that is not a subject for this paper.)

As quickly as the corporate and financial communities develop fraud prevention solutions, enterprising embezzlers find ways around them, requiring the development of a new round of fraud prevention products and techniques.

Alas, the executive who truly wants to protect his or her organization will need to continually update themselves on the latest innovations just to keep the crooks at bay. We wish you the best of luck in that endeavor.

Additional Resources

- ◆ The Association of Certified Fraud Examiners' Report to the Nation 2006 can be downloaded at <http://www.acfe.com/fraud/report.asp>.
- ◆ If you have significant p-card activity, you might want to consider joining The National Association of Purchasing Card Professionals. Go to <http://www.napcp.org/> for additional information.
- ◆ For insights from America's greatest fraud prevention expert, Frank Abagnale, go to <http://www.abagnale.com/index2.asp>.
- ◆ For information about all accounts payable topics, not just fraud, please visit www.ap-now.com.
- ◆ For information about P2P products that utilize technology and help prevent fraud, visit www.baseware.com.

Appendices

Appendix 1: Blank Check Stock Security Features

Changes in the UCC could make organizations liable for fraud against checks if they don't take ordinary care. ANSI standard X9.51 advises the use of at least three security features. Here are some currently on the market. New features are added regularly.

- ✦ ABA Check Endorsement Clause
- ✦ Anti-Splice Backer
- ✦ Copy Void Endorsement
- ✦ Copy-Void in Check Pantograph
- ✦ Covert Fluorescent Fibers
- ✦ Endorsement Warning
- ✦ Fourdriner True Watermark
- ✦ Gradient Two-Color Blend Pantograph
- ✦ Image Friendly Amount Box
- ✦ Fluorescent Fibers
- ✦ Control Numbers
- ✦ Microprinting
- ✦ Multi- Language Chemical Void
- ✦ Non-Negotiable Stub backer
- ✦ Overt Fibers
- ✦ Padlock Security
- ✦ Simulated Watermark
- ✦ Solvent Reactive Color Spotting
- ✦ Thermochromic Ink Toner Adhesion Enhancement
- ✦ Void Pantograph
- ✦ Voidless Postal Window
- ✦ Warning band
- ✦ Watermark Certification Seal

Appendix 2: About Mary S. Schaeffer

Ms. Schaeffer is a nationally recognized accounts payable expert. Following a 15 year career in finance she turned to writing and consulting. For the last ten years she has been researching and writing newsletters for the accounts payable profession. Currently she is the editorial director and publisher of *Accounts Payable Now & Tomorrow*, (www.ap-now.com) a fee-based newsletter published by CRYSTALLUS, Inc. She also directs the firm's consulting endeavors focused primarily on accounts payable issues.

Ms. Schaeffer has an MBA in finance and is the author of over a dozen business books including *Accounts Payable & Sarbanes-Oxley: Strengthening Your Internal Controls*; *The CFO and Controllers' Guide to Accounts Payable*; and *New Payment World: A Manager's Guide to Creating an Efficient Payment Process* to be published in June 2007 by John Wiley & Sons, the publisher of most of her books. Professionals interested in payment issues can sign up for the free weekly e-zine she writes by going to <http://www.ap-now.com/ezinesignup.html>.

Appendix 3: About Accounts Payable Now & Tomorrow and CRYSTALLUS, Inc.

Accounts Payable Now & Tomorrow, (www.ap-now.com), a CRYSTALLUS, Inc. publication, is a monthly newsletter devoted to payment issues. To receive a sample copy of the print publication, send an e-mail to publisher@ap-now.com with the words "BasWare sent me" in the subject line. Make sure you include your company name, title, and mailing address. If you would prefer to just be added to the distribution of the complimentary e-zine, simply send the same information with a note to that effect to publisher@ap-now.com.

In addition to publishing the newsletter, CRYSTALLUS, Inc. provides consulting services to organizations reengineering their accounts payable function. It also works in a collaborative manner with existing staff to develop plans for departmental or payment process improvement. Through an alliance, the firm helps those looking for assistance in recovering duplicate payments. Information on these ventures can be obtained by sending a note to marys@ap-now.com.

APPENDIX 4: ABOUT OUR SPONSOR: BASWARE

BasWare develops solutions that meet customers' needs and contribute to their business success. Founded in 1985, BasWare has over 20 years of experience developing financial software. With over 1,000 clients and 500,000+ users in more than 40 countries, BasWare is the global leader in Enterprise Purchase to Pay solutions. The company is listed on the Nordic stock exchange and growth of net sales on average has been more than 45 percent over the last five years.

BasWare Solutions

BasWare's invoice automation and financial management solutions improve customers' operational efficiency while providing the accuracy, visibility, timeliness, and auditability that enable companies to be compliant and financially agile. BasWare software can also be implemented as a Software as a Service (SaaS) delivery. In addition to software, BasWare offers Business Consulting services to ensure efficient software deployment as well as harmonized procurement and invoicing processes. BasWare's research and development is based on customer needs and general market trends.

Enterprise Purchase to Pay

BasWare Enterprise Purchase to Pay solutions increase the control and management of back-office financial processes, providing tools for procurement, automatic processing of purchase invoices, payment, e invoicing, and archiving. The solutions improve operational efficiency as well as increase transparency of financial operations.

For additional information, please contact BasWare at 203-487-7900

or

www.basware.com/us.

FRAUD IN ACCOUNTS PAYABLE: HOW TO PREVENT IT

For information about this publication

Phone: 302-836-0540

E-mail: publisher@ap-now.com